Microsoft DevOps Solutions: Developing an Actionable Alerting Strategy

ALERTING IN AZURE

John Savill
PRINCIPAL CLOUD SOLUTION ARCHITECT

@NTFAQGuy www.savilltech.com

Learning Objectives

Identify and recommend metrics on which to base alerts

Implement alerts using appropriate metrics

Implement alerts based on appropriate log message

Implement alerts based on application health checks

Analyze combinations of metrics

Develop communication mechanism to notify users of degraded systems

Implement alerts for self-healing activities (e.g., scaling, failovers)

Module Overview

Signals to use with alerting

Types of communication possible

Alerting for self-healing

There will always be times alerting is required for information purposes or to drive action.

It is critical to ensure alerts are used in an appropriate and measured manner to ensure expected response!

Sources of Signals for Alerting

Microsoft Azure Active Directory	Audit Sign-in ...
Subscription	Activity Log
Resources	Metrics Logs
Guest/Extension/ Agent	Metrics Logs

Types of Signal for Alerting

Subscription Activity Log

Includes health and autoscale events

90-day native retention

Azure Monitor Metrics

Native time-series database

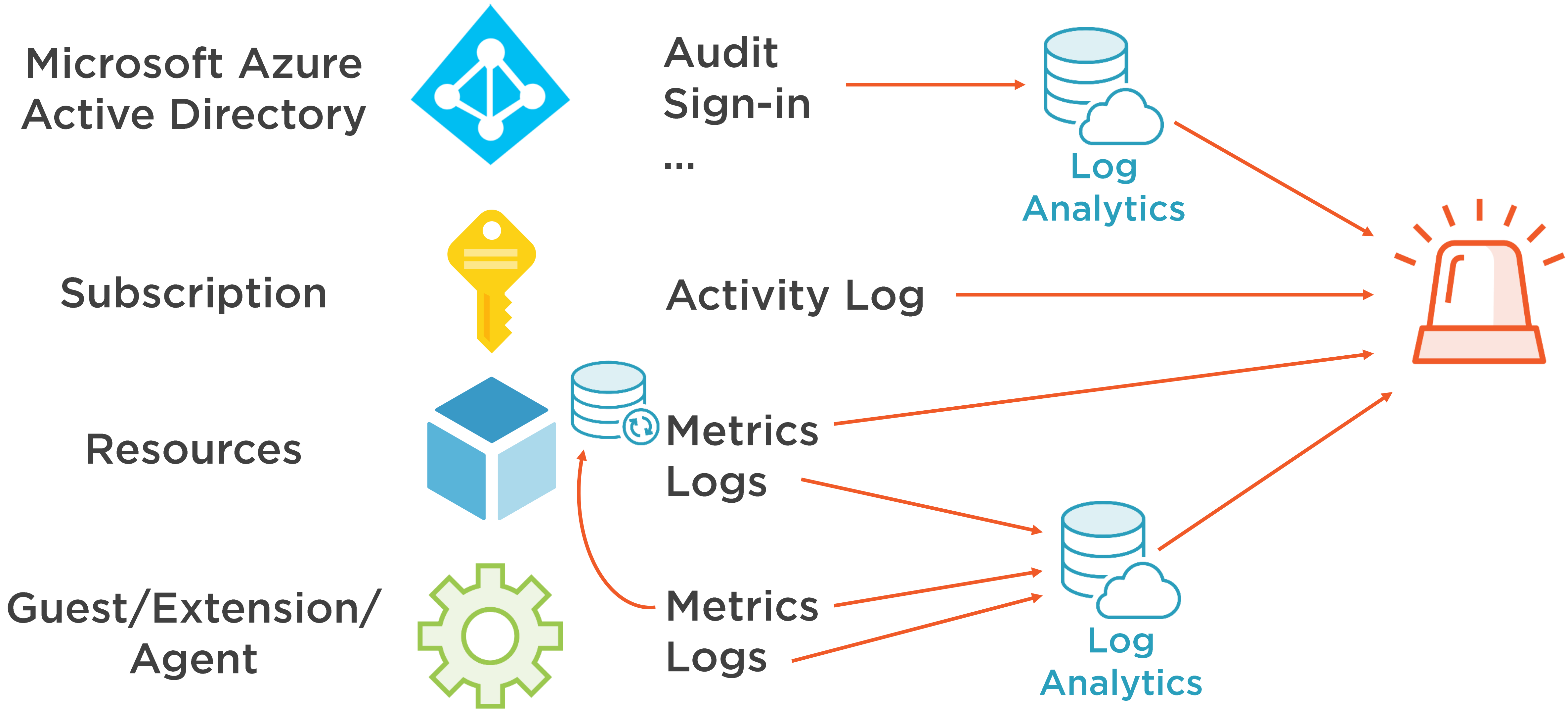
90-day native retention

Log Analytics Log Search

Can be used for storage and query for resource diagnostic logs

Up to 2-year retention

What This Means



Microsoft Azure Active Directory

Audit
Sign-in
...

Log Analytics

Subscription

Activity Log

Resources

Metrics
Logs

Guest/Extension/ Agent

Metrics
Logs

Log Analytics

What Do We Care About?

Every type of Azure resource and service within will have different metrics and logs available

The importance of them will vary by application

It is critical to identify what are the key indicators we care about for performance and failure

Use the Azure Monitor Insights as a starting point to key signals that are important

Use the Topic – Alerts example query set

Autoscale with Azure Monitor

Many services support autoscale

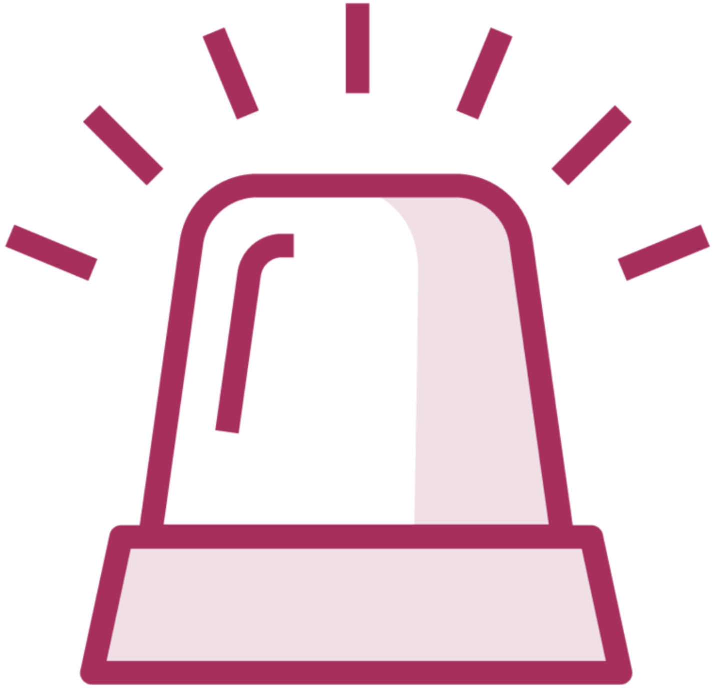
This can help respond to changes in load and the same mechanism can be used to heal

This enables compute to scale based on required amount of work

Azure Monitor enables this behind the scenes

Can alert based on the logs generated

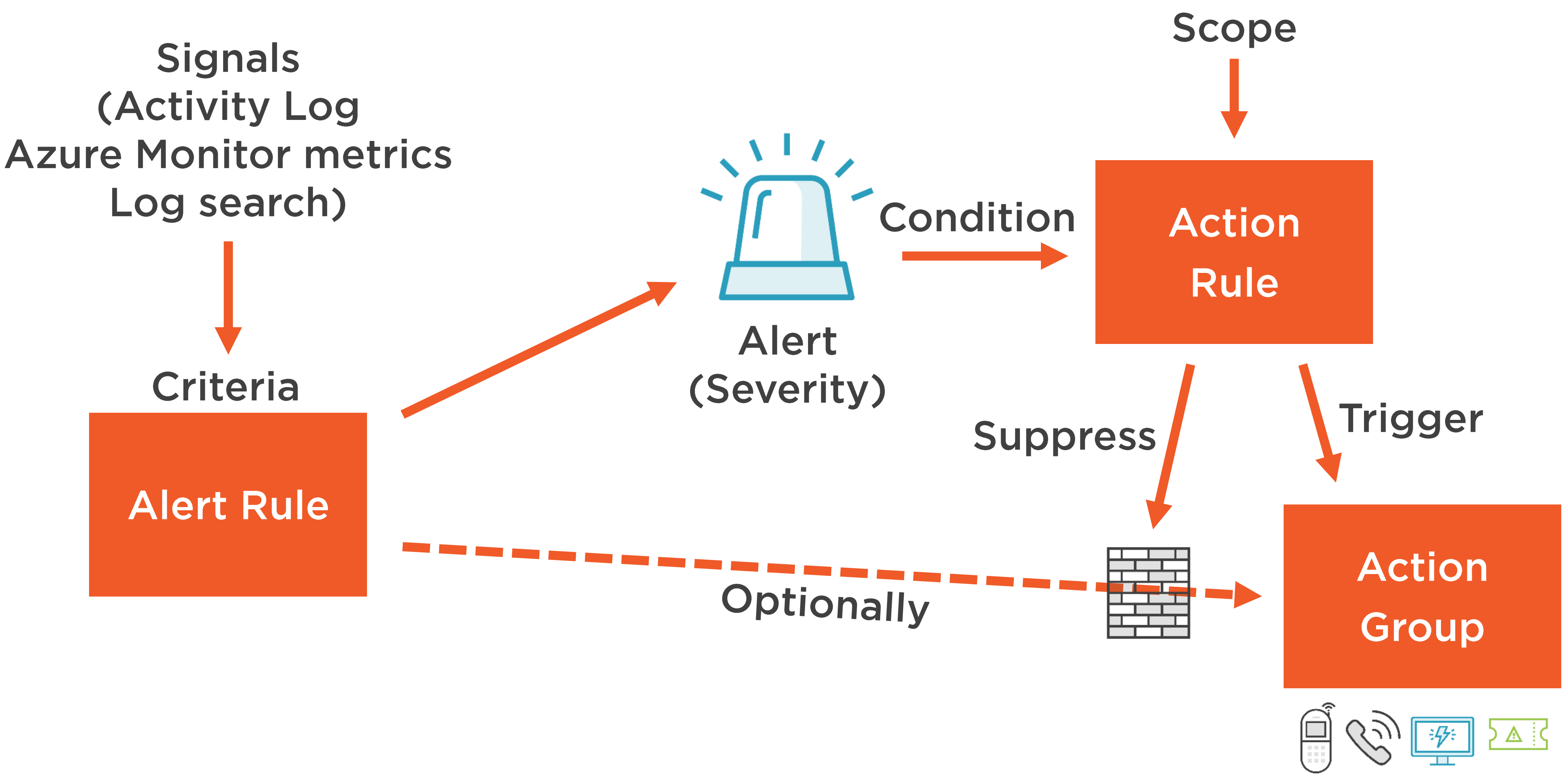
Alerting with Azure Monitor



Azure Monitor provides centralized alerting capabilities built on

- Alert rules
  - Conditions to alert with optional action group
- Action groups
  - Actions to perform
- Action rules
  - Alert conditions to trigger or suppress action group

Alerting Expanded



Communications with Action Groups

There are many options

- Communication based on role assignment or static configuration
- Trigger an action via azure automation, function, logic app, webhook or ITSM
- These actions enable custom communications like Teams/Slack/other interaction

Summary

Signals to use with alerting

Types of communication possible

Alerting for self-healing

Next Up: Creating Custom Dashboards